

SUMMARY
of
GOVERNOR ARNOLD SCHWARZENEGGER'S



**TEAMING UP AGAINST
IDENTITY THEFT:**
A SUMMIT ON SOLUTIONS

CALIFORNIA DISTRICT ATTORNEYS ASSOCIATION
STATE AND CONSUMER SERVICES AGENCY
CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS | CALIFORNIA OFFICE OF PRIVACY PROTECTION

TEAMING UP AGAINST IDENTITY THEFT: A SUMMIT ON SOLUTIONS

Presented by the California District Attorneys Association

SUMMIT ADVISORY COMMITTEE

Charlene Zettel

Director

California Department of Consumer Affairs

Carol Baker

Los Angeles County District Attorney's Office

Bureau of Crime Prevention and Youth Services

Leticia M. Farris

League of California Cities

Roxanne Gould

American Electronics Association

Charles T. Halnan

Direct Marketing Association

Elizabeth Howard

California State Association of Counties

Sheriff Bill Kolender

California State Sheriffs' Association

David LaBahn

California District Attorneys Association

Joanne McNabb

California Office of Privacy Protection

Robert Morgester

California Office of the Attorney General

Thomas O'Connor

Victim Compensation and Government Claims Board

Carol Payne

California Credit Union League

Andrew Roth

California Department of Corporations

Susan Shinneman

eRepublic

Mellonie Yang

California District Attorneys Association

Anissa Yates

California Bankers Association



Arnold Schwarzenegger, Governor

Rosario Marin, Secretary

State and Consumer Services Agency

Charlene Zettel, Director

Department of Consumer Affairs

Joanne McNabb, Chief

California Office of Privacy Protection



GOVERNOR ARNOLD SCHWARZENEGGER

February 23, 2006

Teaming Up Against Identity Theft: A Summit on Solutions

I am pleased to welcome all who have gathered for the Teaming Up Against Identity Theft Summit.

This summit brings together a broad range of citizens – consumers, law enforcement, business and legal professionals, higher education administrators, and state and local government leaders – who are all working to reduce incidents of identity theft.

In addition to facilitating communication among our state's leaders, we must also educate Californians about ways to avoid falling victim to this devastating crime. That is why I increased funding for the California Office of Privacy Protection and enthusiastically support events that raise awareness of this important issue. In recognition of the necessity of public education, this event features prevention workshops that will teach our citizens how to combat identity theft on an individual level.

With the unwavering dedication of concerned Californians, our Golden State will continue to lead the fight against identity theft.

Sincerely,

A handwritten signature of Arnold Schwarzenegger in black ink.

Arnold Schwarzenegger



EXECUTIVE OFFICE
1625 NORTH MARKET BOULEVARD, SUITE S-308
SACRAMENTO, CA 95834
PHONE: (916) 574-8200 ♦ FAX: (916) 574-8613 ♦ INTERNET: www.dca.ca.gov



The attendance of nearly 1,000 at Governor Schwarzenegger's *Teaming Up Against Identity Theft: A Summit on Solutions* demonstrated the high importance that Californians place on privacy protection education and training.

My sincere thanks to Governor Arnold Schwarzenegger, our keynote speakers Deborah Platt Majoras, Chairman of the Federal Trade Commission, and Jan Scully, Sacramento County District Attorney, and to all of our honored guests for endorsing this event. The participation of our excellent workshop instructors and our support team was exemplary.

The Summit was a day filled with successes: success in fulfilling the 2005 Summit recommendations for privacy protection education and successful training in the latest identity theft issues and trends. Attendees filled consumer and Internet safety classes, law enforcement and prosecutor workshops, as well as sessions geared toward higher education, businesses, governments, notaries and the news media. The on-site Victim Clinic provided basic information and, more importantly, real-time advice to those who had fallen victim to identity theft and required support and resources to restore their personal and financial records. Exhibitors reported successful encounters with participants who were actively gathering new resources to enhance privacy protection business practices.

The Summit reinforced the Governor's commitment to a strong privacy protection campaign to educate and protect all Californians. The Department of Consumer Affairs' California Office of Privacy Protection stands ready to respond to the dynamic challenges of identity theft with comprehensive consumer information and targeted education initiatives that will protect consumer privacy and maintain a safe, fair and competitive marketplace for California.

Respectfully,

CHARLENE ZETTEL, Director
Department of Consumer Affairs

TABLE OF CONTENTS

Executive Summary

<i>California Takes on Identity Theft</i>	4
---	---

General Sessions

Teaming Up

Morning Session and Afternoon Session.....	5
--	---

Identity Theft Victim Clinic	5
------------------------------------	---

Summit Attendance.	6
-------------------------	---

Training Workshops

<i>A Summit on Solutions</i>	7
------------------------------------	---

Outgrowth

<i>Future Efforts</i>	10
-----------------------------	----

Appendix.....	11
---------------	----

Executive Summary

CALIFORNIA TAKES ON IDENTITY THEFT

Concerns about identity theft have topped consumer complaint lists across the nation for the last five consecutive years. In January 2006, national researchers noted a leveling off of nationwide statistics at about nine million victims per year; about one million victims are Californians. Yet, the U.S. financial losses increased to nearly \$57 billion in 2005, indicating a higher per-crime incidence.¹

Governor Arnold Schwarzenegger's call to action against identity theft crimes in 2005 resulted in *Locking Up the Evil Twin: A Summit on Identity Theft Solutions*, which assembled panelists from consumer, financial, business and government organizations, law enforcement, and prosecutors. A daylong collaboration in Sacramento on March 1, 2005, helped clarify the major obstacles faced by law enforcement in tackling this crime.

Summit participants recommended increased education and training to restrain these invasive crimes. These recommendations were the basis for the format of the February 23, 2006, conference, *Teaming Up Against Identity Theft: A Summit on Solutions*, held at the Los Angeles Convention Center.

Governor Schwarzenegger opened the Summit's general session, unveiling a higher spirit of commitment to containing crimes of identity theft in California. Morning keynote speaker Deborah Platt Majoras, Chairman of the Federal Trade Commission, relayed the urgency of creating a

national culture of security, and encouraged all stakeholders to become more educated, aware, and able to detect the signs that can lead to identity theft. Sacramento County District Attorney Jan Scully opened the afternoon session with a keynote address focused on California's major metropolitan areas that currently face huge volumes of identity theft cases.

A majority of the event was devoted to twelve individual workshops scheduled at three different times that offered training for consumers, businesses, law enforcement and prosecutors, higher education, government agencies, notaries, and the news media. The variety of courses provided opportunities for attendees to choose topics ranging from basic identity theft protection strategies and current privacy laws affecting business and government to criminal psychology and prosecution challenges.

An on-site Victim Clinic was available to provide real-time support for identity theft victims and interested participants, and an exposition room was available with representatives from companies and organizations that offer identity theft and privacy protection resources.

In follow-up to Summit feedback, the DCA's California Office of Privacy Protection will continue to work with businesses, law enforcement, state agencies and consumer-based organizations to develop general and specific information and educational programs on identity theft and privacy protection.

¹ The Federal Trade Commission (FTC) reported in January 2006 that 2005 was the fifth consecutive year in which identity theft topped the list of consumer fraud complaints received by the Commission, representing 37% of total complaints.

General Sessions

TEAMING UP

MORNING SESSION

The 2006 conference, *Teaming Up Against Identity Theft: A Summit on Solutions* was designed to address education and training needs identified during California's 2005 identity theft summit.

The event was a joint effort of the Schwarzenegger Administration, the California District Attorneys Association, the State and Consumer Services Agency, the California Department of Consumer Affairs, and the California Office of Privacy Protection. Sponsors included Deloitte, eRepublic, the California Victim Compensation & Government Claims Board, Internet Security Systems, the National Notary Association, and Visa.

A Summit Advisory Board representing 16 different state agencies, associations and private industry provided organizational support that contributed to the Summit's success.

About 1,000 attendees were on hand to welcome Governor Arnold Schwarzenegger as he opened the Summit's general session. Governor Schwarzenegger expressed his commitment to protecting privacy and fighting identity theft.

Joining the Governor at the dais were Federal Trade Commission Chairman Deborah Platt Majoras, Senator Charles Poochigian, State and Consumer Services Agency Secretary Rosario Marin, Department of Consumer Affairs Director Charlene Zettel and Los Angeles County District Attorney Steve Cooley.

Federal Trade Commission Chairman Deborah Platt Majoras provided insight to national scale identity theft prevention measures. Chairman Majoras conveyed the need to create a national culture of data security, and for enhanced prosecution and fines that meet the severity of the crime. Majoras encouraged the stakeholders in all aspects of privacy protection to improve their efforts: consumers can become more educated and aware, companies can show leadership through stronger security and protection of personal information, and law enforcement and the legal community can work collaboratively.

AFTERNOON SESSION

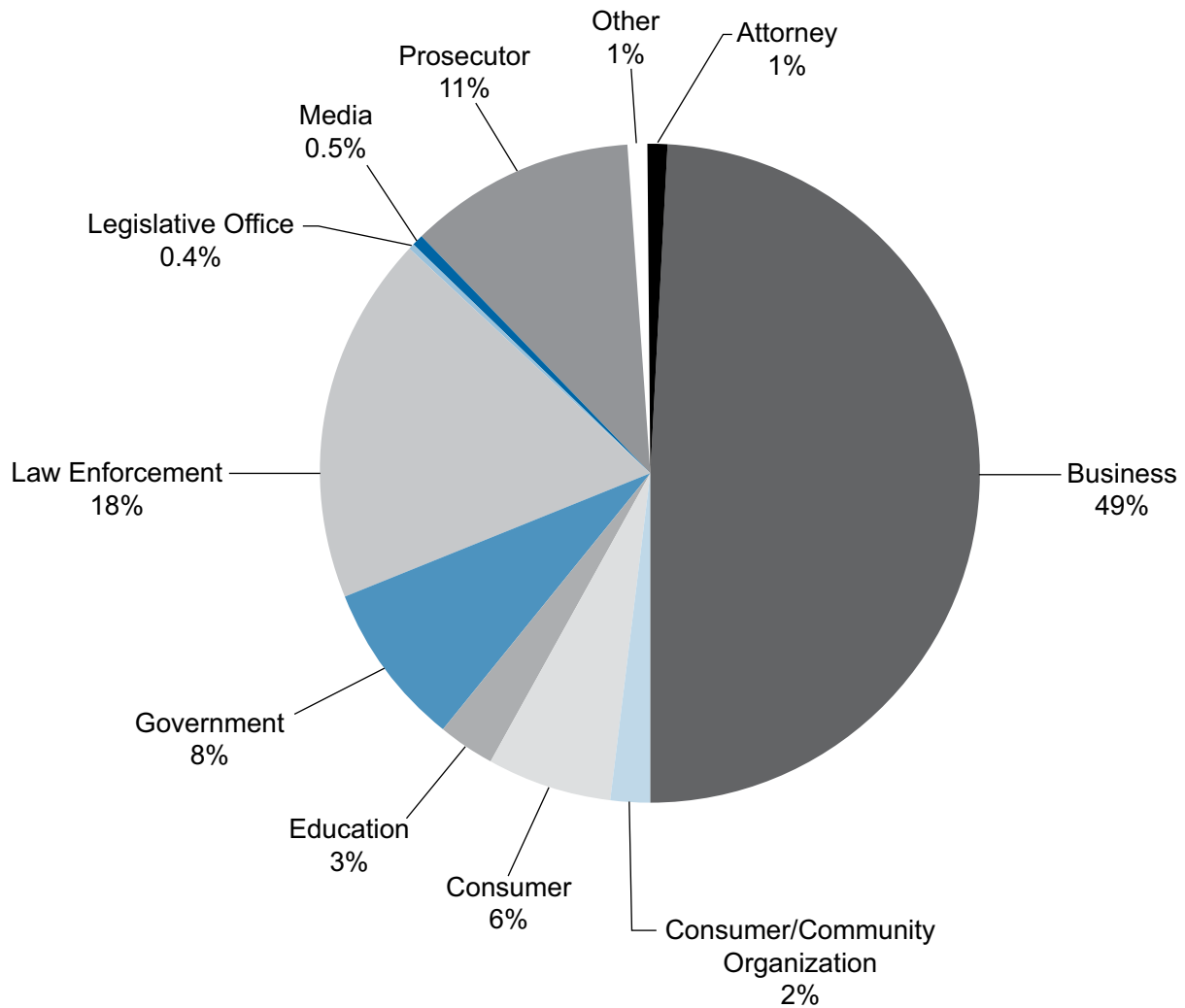
Sacramento County District Attorney Jan Scully presented the afternoon keynote address, discussing numerous cases that highlighted the prevalence of identity theft in everyday life. She noted that statistics continue to show that California has four of the top ten major metropolitan areas in the U.S. with the most identity theft complaints: Los Angeles, San Bernardino/Riverside, the San Francisco Bay Area, and San Diego.

Identity Theft Victim Clinic

A Victim Clinic booth was staffed by the California Office of Privacy Protection, with assistance from the Los Angeles County Department of Consumer Affairs. More than 250 people who visited the booth received on-the-spot answers to their questions about identity theft and helpful information sheets detailing remedial and preventive measures.

2006 Identity Theft Summit

REGISTRANT PERCENTAGES



Summit Attendance

Twelve different workshops were offered in three one-hour segments. Classes were taught by subject matter experts in the areas of consumer protection, business, law enforcement, the legal profession, state and local government, higher education, notary procedures, and background for the news media. Course certification was authorized for law enforcement by the Commission on Peace Officer

Standards and Training (POST); for prosecutors and attorneys, workshops were certified by the California State Bar Association for Minimum Continuing Legal Education (MCLE) credit.

A total of 17 sessions were held throughout the day. The majority of attendees were comprised of businesses, law enforcement, and prosecutors.

Training Workshops

A SUMMIT ON SOLUTIONS

CONSUMER WORKSHOPS

1A-IDENTITY THEFT PROTECTION TIPS FOR CONSUMERS

Instructors: Identity theft victims Mari Frank, attorney and author of books on identity theft; and Jay and Linda Foley, executive directors of the Identity Theft Resource Center

This class was presented twice during the Summit. More than 400 attendees received information and handouts identifying ways to identify warning signs and reduce their risk of becoming identity theft victims. They also learned specific steps to take if victimized by this crime and what to expect during the recovery process. Classes were interactive, with one including an audience participation exercise that tested the participants' knowledge about current identity theft issues.

1B-PROTECTING YOUR PRIVACY ONLINE

Instructors: Cal Poly, Pomona Computer Information Systems students Tom Calabrese, Matthew Kaufman and Michael Wong; radio talk show host Jeff Levy, *Computer Talk*, KNX-1070 News Radio

Offered twice during the day, this course provided more than 200 attendees with techniques to stay safe online and avoid becoming victims of fraud, identity theft, or cyber crime. Attendees gained insight into the online world with information and helpful tips on browsing the Internet, e-mailing and instant messaging, and software downloads, including how to recover from online attacks from viruses and worms. The class included an award-winning educational video on "Phishing," a form of online fraud in which people can be tricked into revealing personal financial information.

LAW ENFORCEMENT WORKSHOP

2-IDENTITY THEFT INVESTIGATION

Instructors: Investigator Jerry Camp, Computer and Technology Crimes High-Tech Response Team (CATCH); Detective Dave Shriver, Southern California High Tech Crimes Task Force

The three segments of this all-day course were restricted to law enforcement officers and prosecutors. The course was taught by experienced investigators from the identity theft detail of two Southern California High Tech Crimes Task Forces, and was POST-accredited. Nearly 200 officers gained basic techniques and strategies for investigating identity theft, which include taking initial complaints, handling jurisdictional issues, working with the victim, and procedures for patrol officers. Special attention was given to the difficulties investigators and prosecutors face due to jurisdictional constraints and time lags in the victim's discovery and reporting of the crime. Officers learned how to spot the signs of identity theft during the investigation of other crimes and were encouraged to assist the victim in obtaining and providing copies of documents associated with fraudulent accounts.

PROSECUTOR WORKSHOPS

3A-IDENTITY THEFT PROSECUTION 101

Instructors: Los Angeles County District Attorney Jeff McGrath, Riverside County District Attorney Charles Chaiyarachta

As participants of the Southern California High Tech Crimes Task Force, the instructors designed this class specifically for prosecutors and law enforcement personnel who are assigned to identity theft case review, filing, and prosecution. Topics included bail, filing, and charging techniques.

Instructors discussed ways to overcome barriers to prosecution and parallel offenses that are often associated with identity theft. Eligible attendees earned one hour of California MCLE credit.

3B-PROSECUTING THE IDENTITY THEFT RING

Instructors: Los Angeles County District Attorney Jonathan Fairtlough, Santa Clara County Deputy District Attorney James Sibley, REACT Task Force member and Santa Clara County Deputy District Attorney Bud Frank

It can take thousands of man-hours to prosecute large-scale identity theft cases. Course instructors used examples from the 2005 ChoicePoint and Accurant cases to illustrate their discussion on prosecuting large-scale cases that require the collection of evidence that is sometimes difficult to obtain, and the orchestration of several parties before taking the matter before the courts. Instructors discussed the complexities of prosecuting a case in which direct witnesses are scarce and business records offer the only proof. Eligible attendees earned one hour of California MCLE credit.

BUSINESS AND MERCHANT WORKSHOPS

4-BUSINESS PRACTICES FOR PREVENTING IDENTITY THEFT

Instructors: Chief of the California Office of Privacy Protection Joanne McNabb, Privacy Compliance Group, Inc. Chief Executive Officer Gary Clayton

Increases in identity theft in recent years have raised consumer concern about how the companies they do business with handle their personal information. Offered twice during the summit, this class provided more than 200 business owners and managers with an overview of privacy laws for businesses and on best practices for managing personal information. Attendees learned about the risks and obligations of handling sensitive information, as well as safeguards to protect customers and employees from identity theft. Attendees received a copy of

A California Business Privacy Handbook published by the California Office of Privacy Protection.

5-PAYMENT CARD SECURITY FOR MERCHANTS

Instructors: Visa USA, Inc. Fraud Control Vice President Joseph Majka, Deloitte Senior Manager Kieran Norton

When customers use their payment cards at the point of sale, over the Internet, on the phone, or through the mail, they want assurance their account information is safe. These customer expectations resulted in a collaboration of the major payment card companies and issuance of the Payment Card Industry Data Security Standard and its guiding principles. About 150 participants learned about the “digital dozen” requirements that merchants who accept payment cards must follow, including building and maintaining a secure network with strong access control measures, and regular monitoring and testing of network security. The instructors also discussed security breach notification laws enacted in many states during 2005 as a result of several major security breaches that affected millions of Americans.

NEWS MEDIA WORKSHOP

6-BACKGROUND ON CALIFORNIA LAWS ON PRIVACY AND IDENTITY THEFT FOR MEDIA

Instructors: DCA Office of Public Affairs Chief Russ Heimerich, DCA Staff Counsel Dana Winterrowd

An overview of California’s privacy laws for news media and other communication professionals helped explain the legal and practical use of personal information about subjects that are reported on in the daily news. Instructors defined what constitutes identity theft and consumer rights under current state and federal law. Emerging identity theft methods and privacy protection obligations of merchants and data collection companies also were covered. Attendees were provided with resource materials to assist them when developing identity theft or privacy protection stories.

LEGAL WORKSHOP

7-CALIFORNIA PRIVACY AND IDENTITY THEFT LAWS FOR ATTORNEYS

Instructors: DCA Staff Counsel Dana Winterrowd; Sonnenschein, Nath & Rosenthal, LLP Partner Reece Hirsch

More than 400 legal professionals registered to hear summaries of legislative, regulatory and common law developments, together with compliance suggestions and instructive histories of identity theft cases. This class included a review of recent California laws relating to security breach notification, reasonable security measures, financial privacy, online privacy notices and direct marketing disclosures. Eligible attendees earned one hour of California MCLE credit.

HIGHER EDUCATION WORKSHOP

8-IMPROVING PRIVACY AND SECURITY AWARENESS ON CAMPUS

Instructors: Information Security Officer and Physics Professor Dr. Javier Torner, CSU, San Bernardino; Information Security Systems Professor, Dr. Dan Manson, Cal Poly, Pomona

Colleges and universities have been among the hardest hit in recent years by computer hackers and identity thieves. During this course, instructors explained how some universities are actively accelerating and implementing both campus security awareness programs and protected information storage systems through grants and studies that address the theft and breach issues. Discussion included challenges and successes when developing strategies, activities, and effective communication to a diverse academic audience. Attendees received valuable information and resources needed to implement an effective security awareness program in a university environment.

GOVERNMENT AGENCY WORKSHOP

9-PRIVACY PRACTICES FOR GOVERNMENT AGENCIES

Instructors: Chief Information Security Officer Kevin Dickey, Contra Costa County, California; California Office of Privacy Protection Chief Joanne McNabb

The heightened importance of privacy for government agencies in recent years is tied, in part, to the widespread use of portable computers and data storage media, and an increasing role of the Internet in providing service to citizens. In this class, about 150 government representatives received an overview of new state and federal privacy laws that apply to government agencies, and best practices for protecting personal information in government agencies, including tips on responding to security breach incidents.

NOTARY WORKSHOP

10-IDENTITY THEFT PREVENTION FOR NOTARIES

Instructor: Educational Services Instructor Kate Donovan, National Notary Association

As identity thieves become more sophisticated, the job of the notary public becomes more challenging. By verifying identity, ascertaining the willingness and awareness of signers, and authenticating signatures, the notary safeguards personal identification and provides invaluable protection against fraud. This class provided notaries with practical methods that can help prevent problems on the spot. Class materials included effective tools that provide notaries with the confidence necessary to better protect themselves and the people they serve. Demand for this class was high; it was offered twice and was attended by more than 400 notaries.



Outgrowth

FUTURE EFFORTS

Governor Schwarzenegger's 2006 Identity Theft Summit delivered a consistent message of the need for enhanced statewide education and training programs that will help construct a shield of protection to control this crime.

The Department of Consumer Affairs' California Office of Privacy Protection will continue to develop and present focused training workshops

throughout the State. These workshops will address both general and specific aspects of identity theft and privacy protection that arise in the marketplace.

The next statewide identity theft summit is planned for March 2007. Information on this event and links to the California Office of Privacy Protection's spectrum of information, education and protection guides can be accessed at www.idtheftsummit.ca.gov.

Appendix

REMARKS OF CHAIRMAN DEBORAH PLATT MAJORAS² TEAMING UP AGAINST IDENTITY THEFT: A SUMMIT ON SOLUTIONS

I. INTRODUCTION

Thank you. I am pleased to be here for California's second summit on identity theft. I thank Charlene Zettel, Director of the California Department of Consumer Affairs for inviting me, and I applaud the State's leadership in this area. The State of California and the Federal Trade Commission share a common goal and a clear commitment to identity theft prevention and victim assistance.

Identity theft is a particularly pernicious crime requiring swift action on many fronts. Like a virus, it spreads through our economic system, striking randomly and often inflicting great harm on innocent victims. According to a San Jose, California, consumer who called the FTC's consumer help line, in just one day identity thieves opened nine credit card accounts in her name and incurred \$15,000 in charges. Unfortunately, this victim's tale is not unusual—and it is far from the most egregious case.

The theme for today's Summit is "teaming up" and that is perfect. Vince Lombardi, America's "prophet" on teamwork, said, "People who work together will win, whether it be against complex football defenses, or the problems of modern society." In an era when it is fashionable to categorize issues as federal, state, or local, identity theft stands out as genuinely requiring a coordinated response at all levels. Officials at all levels of government, the private sector, and consumers all play critical roles in this fight, and the whole is greater than the sum of its parts. As Mr. Lombardi said: "Individual commitment to a group effort—that is what makes a team work, a company work, a society work . . ."

II. THE ROLE OF GOVERNMENT

State and local officials, district attorneys, and police departments provide the offense. They are the primary players in tracking down and prosecuting identity thieves and in providing their victims with assistance in reclaiming their identities, and their experience provides invaluable insights to all who work together to solve this difficult problem. While these are sometimes complex cases to investigate and prosecute, criminal law enforcement authorities are persevering and putting these thieves behind bars where they belong. One such thief who we will not be hearing from for a long time is Mr. Oluwatosin, who was just sentenced to 10 years imprisonment and ordered to make restitution of \$6 million as part of the ongoing criminal investigation involving data broker ChoicePoint.³ This case, which was investigated by the Los Angeles County District Attorney's Office and Sheriff's Department, as well as several federal agencies, is a prime example of successful teamwork.

State and local agencies also provide the first helping hand to victims, who often turn first to their local police departments or state consumer protection agencies for assistance. State and local governments are especially well-positioned for this role because they can provide their residents with victim assistance that is tailored to their needs.

Because state and local government are on the front line, they also have been innovators in developing new ideas for tackling identity theft. The California law requiring consumer notice after certain types

² The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any other Commissioner.

³ See Los Angeles County District Attorney's Office press release "Nigerian Gets 10 Years Prison; Must Pay \$6.5 Million in Identity Theft Case" (Feb. 10, 2006), available at http://da.co.la.ca.us/mr/021006a.htm?zoom_highlight=+Oluwatosin.

of data breaches, for example, has raised awareness about the issue of data security and brought about important changes.

III. THE ROLE OF THE FEDERAL TRADE COMMISSION

The federal government also is playing a strong role in the fight against identity theft. At the FTC, we take seriously our responsibility to promote a coordinated framework for attacking a national problem; vigorously enforce consumer protection laws related to identity theft and data security; assist criminal law enforcement authorities in bringing identity thieves to justice; assist victims in recovery; and educate consumers and businesses.

A. FTC ENFORCEMENT

Americans' concerns about the security of their personal data and their risk of identity theft have spiked with recent reports about data breaches. The FTC's aggressive law enforcement program, using our full arsenal of statutory tools, targets companies that fail to implement reasonable measures to protect sensitive consumer information.

One of the FTC's most recent law enforcement actions arose from ChoicePoint's high-profile breach that occurred last year and was reported pursuant to California law. In our complaint, we allege that consumer data broker, ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of the Fair Credit Reporting Act (FCRA)⁴ and the FTC Act.⁵ For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. According to our complaint, ChoicePoint's failures allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. The FTC alleged that at least 800 cases of identity theft arose out of these incidents. The Commission obtained \$10 million in civil penalties for the FCRA violations—the highest civil penalty ever levied in a consumer protection case—\$5 million in consumer redress for identity theft victims, and significant injunctive provisions that require ChoicePoint to implement a variety of new data security measures. This settlement is an important victory for consumers and also an important lesson for industry.

The ChoicePoint settlement follows on a dozen security cases against household names like Microsoft, DSW Shoe Warehouse, BJ's Wholesale Club, and others. In some of these cases, we alleged that the

⁴ 15 U.S.C. §§ 1681-1681x.

⁵ *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (complaint and proposed settlement filed on Jan. 30, 2006 and pending court approval). *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (March 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

companies made false promises to take reasonable steps to protect sensitive consumer information.⁶ In others, we alleged that the failure to take reasonable security measures to protect sensitive customer data was an unfair practice in violation of the FTC Act.⁷ And in a third group of cases, we alleged violations of federal rules under the Gramm-Leach-Bliley Act (GLBA)⁸ requiring “financial institutions” to implement safeguards for their data.⁹ No matter what the source of our legal authority, these cases all stand for the proposition that record keepers must protect sensitive consumer information.

And just this morning, to reinforce that message, the Commission is announcing a settlement with CardSystems Solutions, Inc., the processor allegedly responsible for the Visa and MasterCard breach last year affecting tens of millions of credit and debit cards.¹⁰ This case addresses the largest known compromise of financial data to date. Here again, the FTC alleged that CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer data. The settlement requires CardSystems and its successor corporation to implement a comprehensive information security program and obtain audits by an independent third-party professional every other year for 20 years. As noted in the FTC’s press release, CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.

The ultimate goal here is not to rack up more settlements and fines. That is not how we will measure our success. Rather, the goal here is to create a culture of security for sensitive information so that businesses prevent breaches and identity theft. Our cases make plain that they first must implement reasonable data security practices to keep sensitive consumer data such as Social Security numbers from falling into criminal hands. The laws and rules we enforce do not require that information security be perfect. That would be a costly, unobtainable standard. Rather, we require that a company’s data security be reasonable in light of the nature of its business and the sensitivity of the information it handles. That is “Data Security 101.” Consumer information is the currency of our information economy. Just as we know that businesses keep their cash safe, we must insist that they keep consumers’ sensitive information safe.

In addition, businesses must implement strong fraud prevention measures to prevent identity thieves from using consumer information to perpetrate fraud. For example, by using strong authentication measures, a business can ensure that a person is who he or she purports to be, and thus spot and screen out potential identity thieves.

⁶ *In the Matter of BJ’s Wholesale Club, Inc.*, FTC Docket No. 042-3160 (Sept. 20, 2005); *In the Matter of DSW, Inc.*, FTC Docket No. 052-3096 (proposed settlement posted for public comment on Dec. 1, 2005). Documents related to the enforcement action against BJ’s Wholesale Club are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html. Documents relating to the enforcement action against DSW are available at <http://www.ftc.gov/os/caselist/0523096/0523096.htm>.

⁷ 15 U.S.C. § 6801-09.

⁸ 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16.

⁹ C.F.R. Part 314 (“Safeguards Rule”). *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005); *Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (April 12, 2005); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005).

¹⁰ *In the Matter of Card Systems Solutions, Inc. and Solidus Networks, Inc., d/b/a Pay by Touch Solutions*, 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006).

Many companies already have shown leadership on these fronts, and we applaud them. We also commend industry for working to assist identity theft victims through, for example, the Identity Theft Assistance Center, or ITAC as it is known, which was established by major banks to work one-on-one with victims to resolve their problems. Still, some companies have failed to implement even basic information security measures that can be implemented at relatively low cost, such as developing a security plan, training employees about data security issues, and overseeing service providers that have access to sensitive customer data. In our cases, for example, we alleged that some of the companies failed to defend against common, well-known Web attacks; some stored credit card data when they had no business need to do so; and some stored sensitive data in files that could be accessed easily by using commonly known default user IDs and passwords. The consent orders settling these cases require the companies to implement comprehensive information security programs and obtain third party audits.¹¹

If the law enforcement message is not enough, companies must realize that inadequate security is just bad business. A Visa International survey of more than 6,000 consumers across 12 countries, conducted following some of the recent high-profile data breaches, found that data security was a major concern for 64% of respondents. The survey also found that consumers changed their behavior due to fears about identity theft, with 24% reporting that they limited use of online shopping sites.¹² Similarly, a survey by the Ponemon Institute found that, of the respondents who had received a letter notifying them of a data breach, 58% said it decreased their trust and confidence in the organization.¹³ These surveys make clear that providing appropriate protections for sensitive consumer information is good business.

B. FTC OUTREACH

Outreach to and among businesses, consumers, and law enforcement is critical. The 1998 Identity Theft Assumption and Deterrence Act (“the Identity Theft Act”) assigned the FTC a unique role in

¹¹ In addition to our law enforcement efforts, we also have an active rulemaking program to implement provisions of the Fair and Accurate Credit Transactions Act of 2003, or FACT Act, related to identity theft. The FACT Act requires the FTC, alone or in conjunction with other agencies, to adopt 18 rules, undertake eight studies, and conduct three consumer education campaigns. To date, we have completed eleven rules or similar obligations, proposed two additional rules, published five studies, and completed one consumer education campaign with two others in progress.

In 2005, the FTC issued a final rule requiring businesses that make firm offers of credit or insurance to consumers, often called “prescreened offers,” to provide enhanced disclosures of consumers’ right to opt out of receiving such offers. 16 CFR 642 and 698 App. A (70 Fed. Reg. 5022; Jan. 31, 2005). See “FTC Prescreen Opt-out Notice Rule Takes Effect August 1” (July 27, 2005), available at <http://www.ftc.gov/opa/2005/07/prescreenoptout.htm>. In addition, the FCRA requires all businesses and individuals who use consumer reports to take reasonable steps to dispose of the reports once they are done with them. 15 U.S.C. § 1681w. The purpose of this requirement, which is embodied in the so-called Disposal Rule, is to protect against unauthorized access to the reports, such as when identity thieves troll for sensitive information left in dumpsters. Perhaps most importantly, the FACT Act gives consumers nationwide the right to a free annual credit report. 15 U.S.C. § 1681j(a)(1).

Our FACT Act work is not yet done. The Commission is working with the bank regulatory agencies to develop the so-called “Red Flags” Rule that requires financial institutions and creditors to spot signs of identity theft. 15 U.S.C. § 1681m.

¹² See Visa press release “Technology, Cross-industry Collaboration Key to Enhancing Security” (Jan. 25, 2006), available at <http://corporate.visa.com/md/nr/press280.jsp?src=home>.

¹³ See Consumer Affairs press release “Data Breaches Bad for Business” (Sept. 27, 2005), available at http://www.consumeraffairs.com/news04/2005/data_breaches_business.html. Nineteen percent said they immediately terminated their accounts with vendors who lost the information; 40% considered taking their business elsewhere; and 5% said they hired lawyers.

combating identity theft and coordinating government efforts.¹⁴ Thus, in addition to law enforcement, the Commission's program includes business education to promote better security practices; consumer education and victim assistance; and coordination with other law enforcement through the Identity Theft Data Clearinghouse, a centralized database of victim complaints.

Our business outreach efforts include providing guidance on issues related to data security. For example, the Commission has disseminated guidance for businesses on reducing risks to their computer systems,¹⁵ as well as guidance on complying with the GLBA Safeguards Rule.¹⁶ We also have published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, a business education brochure on managing data compromises.¹⁷ This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

Finally, the FTC operates the Identity Theft Data Clearinghouse, the nation's central database of victim complaints designed to support law enforcement investigations nationwide. The database includes over one million complaints received directly from consumers as well as various state and federal agencies. It enables us to gain a better understanding of how identity theft is afflicting consumers and serves as a resource for over 1,300 law enforcement agencies, more than 100 of which are California law enforcement agencies.

To encourage greater use of the Clearinghouse, the FTC staff offers seminars to law enforcement across the country. Teaming up with the Department of Justice, the U.S. Postal Inspection Service, FBI, the American Association of Motor Vehicle Administrators, and the U.S. Secret Service, the FTC has thus far conducted 19 seminars involving more than 2,780 officers from over 980 different agencies. This spring, the FTC and our training partners will conduct three such training sessions across California. The FTC staff also developed an identity theft case referral program, which examines patterns of identity theft activity in the Clearinghouse and then makes referrals to identity theft task forces around the country. Overall, the Clearinghouse is one of our best examples of how we can work together to combat identity theft.

IV. THE ROLE OF CONSUMERS

The undisputed MVP on the ID theft prevention team is the educated consumer. Education empowers, and nowhere is it more important than in the fight against identity theft.

As many of you may know, the Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft. We receive over 15,000 contacts per week from victims and consumers who want to avoid becoming a victim. Callers to the hotline receive counseling from trained personnel (including Spanish-speaking personnel) who, for example, advise victims to obtain their credit reports, request a fraud alert, contact creditors, and file a police report. The FTC's hotline is not the only place consumers can find counseling, however. Here in California, for example, the Identity

¹⁴ Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

¹⁵ See Security Check: Reducing Risks to Your Computer Systems, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/security.htm>.

¹⁶ See Financial Institutions and Customer Data: Complying with the Safeguards Rule, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>.

¹⁷ See Information Compromise and the Risk of Identity Theft: Guidance for Your Business, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/idthespond.pdf>.

Thrift Resource Center and the Privacy Rights Clearinghouse have implemented stellar victim assistance programs.

The Commission also has developed and distributed step-by-step guides on how to avoid identity theft and how to deal with its effects.¹⁸ These, and other materials, can be found on the FTC's dedicated identity theft website.

We also have launched a number of efforts to simplify the victim recovery process. FTC staff worked with industry and consumer groups to develop an ID Theft Affidavit, a standard form for victims to use in resolving identity theft debts. This Affidavit has saved time for victims who previously often had to fill out multiple fraud affidavits. Now, our staff is working with the International Association of Chiefs of Police and industry and consumer groups on developing a universal police report for identity theft. Police reports are key to victim recovery because they show that identity theft has occurred and can serve as an "identity theft report" for the purpose of exercising certain new rights under the FACT Act.¹⁹ They can, however, put an enormous strain on police department resources. The universal identity theft report would allow victims to complete a report at the Commission's website and take it to their local police department, where a police officer could verify the report through a victim interview and then provide confirmation to the FTC. It should simplify the recovery process for victims, lessen the burden on police departments, and provide assurances to companies that the information in the report is reliable.

Recent surveys demonstrate both progress and challenges in educating consumers. For example, the Visa International survey found that 63% of consumers say they are now more careful when disposing of financial statements and 62% say that they have become more discriminating about the sites at which they make purchases.²⁰ On the other hand, a recent survey conducted by the National Cyber Security Alliance found that over half of the respondents either had no anti-virus protection or had not updated it within the past week, about half did not have a firewall, and 40% had no spyware protection. Yet, 83% said they were "safe from online threats." Of the respondents who had received a phishing e-mail, 70% of those thought the phishing e-mails were from a legitimate company.²¹

These results tell me that government at all levels needs to re-double our efforts at educating consumers on how to protect their personal information. We continuously must work together to develop new, creative ways to get our messages out. Last fall, the FTC, together with partners from law enforcement, the technology industry, and nonprofits, launched OnGuard Online, an interactive, multi-media resource for

¹⁸ See ID Theft: What It's All About, available at <http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.pdf> and Take Charge: Fighting Back Against Identity Theft available at <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm>. Since February 2002, the FTC has distributed more than 1.9 million copies of the Take Charge booklet and recorded more than 2.3 million hits to the Web version.

¹⁹ These include the right to an extended, seven-year fraud alert, the right to block fraudulent trade lines on credit reports, and the ability to obtain copies of fraudulent applications and transaction reports. See 15 U.S.C. § 1681 et seq., as amended.

²⁰ See *supra* note 11.11.

²¹ See "AOL/NCSA Online Safety Study" (Dec. 2005), available at http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

information and up-to-the minute tools on how to recognize Internet fraud, avoid hackers and viruses, shop securely online, and deal with identity theft, spam, phishing, and file-sharing.²²

And this spring, the FTC will launch a substantial new identity theft campaign to show consumers how to minimize their risk of falling victim to identity theft. The campaign will encourage consumers to “Deter, Detect, and Defend” against identity theft by taking steps to reduce their risk, keep a close eye on their personal information, and move quickly to minimize the damage if identity theft occurs. The centerpiece of the campaign is a turnkey toolkit—a comprehensive how-to guide on providing consumer education about identity theft. The toolkit, which includes everything from PowerPoint presentations to pamphlets, will empower consumers to educate each other on identity protection.

We recognize that, in developing all of these programs, it is important to have a clear understanding of the nature, extent, and prevalence of our adversary—identity theft. Although consumer complaints provide some information about these issues, the Commission has given a priority to collecting supplemental evidence through consumer surveys. We currently are conducting a new national identity theft survey, which should reveal any changes and new trends since our first survey in 2003.²³

V. CONCLUSION

Unlike professional football, identity theft does not have an off season. Together, we must combat identity theft 365 days per year. I understand that the heavy-lifting on this front is being done by state and local law enforcement. That being said, there are a number of ways that we can partner as we move forward. First, I encourage every organization, whether a government agency, consumer group, university, or business to share the ID theft prevention tips at OnGuardOnline.gov with employees, customers, students, members, and constituents. OnGuard Online is branded independently of the FTC, so that your organizations can make the website and the important information your own. Second, I encourage each of you to file comments and participate in the FTC’s ongoing FACT Act rulemakings. Third, I hope that all of the law enforcement agencies participating in today’s summit also will join the FTC at the three upcoming identity theft seminars to be held here in California this spring. And finally, I hope that every law enforcement agent will take advantage of the Identity Theft Data Clearinghouse, an invaluable resource. You can get more information about obtaining free access to the Clearinghouse and the upcoming seminars at the FTC’s booth located in the Summit exhibitor room.

I thank Governor Schwarzenegger and his Office of Privacy Protection for organizing this important summit, and the California District Attorneys Association for hosting it. Thank you.

²² See www.onguardonline.gov.

²³ See Federal Trade Commission – Identity Theft Survey Report (Sept. 2003), available at <http://www.ftc.gov/os/2003/09/synovatoreport.pdf>.

SACRAMENTO COUNTY DISTRICT ATTORNEY JAN SCULLY TEAMING UP AGAINST IDENTITY THEFT: A SUMMIT ON SOLUTIONS

TIGER WOODS CASE:

Good Morning everyone, we're here today to spend some time talking about Identity Theft. None of us are immune from victimization. Twelve years ago, it took me over a week to realize that the only person getting mail in our mailbox was my husband. By the time I recognized it, new credit card accounts had been opened up in my name and charges were already accruing. But, enough about me. As a prosecutor, I love to talk about cases.

Consider the case of Anthony Taylor. Prosecuted by my office just a few years ago, Taylor had a criminal record of 20 convictions, going back to the age of 14. At age 20, he had been convicted of two counts of home invasion robbery. But after serving his prison time, he learned that he could make much more money, without the physical danger, by going white collar. So in 1999, he located the Social Security number of a man he had never met, got a driver's license in that man's name—Eldrick T. Woods—and then used this information to go on a buying spree. He went into stores offering “instant credit,” and bought furniture. At Good Guys he got electronics equipment. Putting just \$100 down because of his good credit, he drove away from the dealership with a used Lexus.

It was easy, because when the computer check was done against the name of Eldrick T. Woods, with that Social Security number, he had excellent credit. And well he might. You probably have heard of Eldrick by another name—Tiger Woods, golfer extraordinaire, Sports Illustrated's Athlete of the Year, and corporate spokesman for Disney, Nike sportswear, Rolex watches, American Express Credit Cards, and Buick Automobiles.

In just a short time Mr. Taylor—who was on parole—netted \$17,000 in merchandise and services. He was caught when a routine parole search turned up some of the property. Of course, an avid golf fan might have picked up the clues sooner, but while most people recognize the golfer Tiger Woods, not many would recognize the name Eldrick. Tiger hadn't been in Sacramento recently, as my deputy established when Mr. Woods was on the witness stand—not since he was 13 years old, when he competed in a junior golf tournament (which he won). When asked on the witness stand if he had bought that used Lexus, and being the good spokesperson he is, Tiger answered, “No. Are you sure it wasn't a Buick?”

Anthony Taylor, aka Eldrick Woods, was convicted under the Three Strikes law because of his prior home invasion robberies and received a life sentence. But his \$17,000 take represents, by the standard of some identity thieves, only a modest haul.

THE CURRENT PROBLEM OF IDENTITY THEFT:

As was discussed in the morning session, the number of identity theft victims is staggering. Even though a large number of individuals have already been victimized, the number of victims continues to grow.

Background Information

- A report released last month by the Federal Trade Commission shows just how big the identity theft problem is. The Consumer Sentinel database, maintained by the FTC, collects information about consumer fraud and identity theft complaints from over 150 organizations.
- In 2002, the database recorded 161,896 identity theft complaints. By 2004, that number climbed to 246,570.

- The number of identity theft complaints has increased steadily, with a total of 255,565 identity theft complaints in 2005.
- Credit card fraud continues to be the largest single category of identity theft, accounting for 26% of the complaints. Also high on the list are phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%).

IDENTITY THEFT IN CALIFORNIA:

Identity theft continues to be a significant problem in California. In raw numbers, California is far ahead of any other state. Four of the top ten major metropolitan areas in the United States with the most identity theft complaints per 100,000 people are in California. These are:

1. Los Angeles
2. San Bernardino/Riverside “Inland Empire”
3. San Francisco Bay Area
4. San Diego

In the Los Angeles area alone there were over 3,600 complaints last year. This actually represents an improvement over 2004 when California had five metropolitan areas in the top ten. (The Sacramento area, the fifth metropolitan area, was ranked fourteenth in complaints for 2005.)


PARTNERSHIPS:

Identity thieves are working hard to get your personal information and are continually developing new scams. These criminals are generally one step ahead because identity theft is easy to commit, hard to detect, and has only minimal criminal penalties. It is imperative for law enforcement and other public safety partners to continually find out what new scams are being used in order to detect scams and fight back.

An example of just how creative these thieves have become came from an incident earlier this month in the Central Valley, when two men were arrested for taking part in a debit card theft ring. While the theft of debit card information is nothing new, the manner in which they acquired it is. Debit card information was stolen from customers at automated teller machines and gas stations using a sophisticated combination of one-way mirrors, miniature cameras, and magnetic strip readers. Plastic coverings, that contained a card reader, were placed over magnetic strip readers at ATMs and payment kiosks at gas stations. The card reader captured debit card information while still allowing unsuspecting customers to proceed with their transaction. Using a mini-camera hidden inside a mirror mounted on the machine, these thieves were able to capture the user's PIN number.

To meet the challenge that identity theft poses, we need to be just as creative as the criminals, thinking in new ways about how we approach law enforcement. We need to identify the criminal trends, so that we can stay one step ahead of the crooks, and give Anthony Taylor some company in prison, as he rues the day he decided to target the identity of Eldrick Tiger Woods.

Because so many identity theft crimes are multi-jurisdictional, we must not only think multi-jurisdictional, we must act multi-jurisdictional. We must work together not only in identifying and apprehending the thieves, but also in creating new education and prevention strategies, within the law enforcement



community, and in partnership with the business community, especially our financial institutions, and consumer advocates. But, we need to go even further than that. When it comes to identify theft, instead of businesses and consumers being at different ends of the sales transaction, they need to work side by side to prevent and minimize the ever-sophisticated criminal enterprise that keeps all of us on our toes. Working together, we can rise to the challenge of this criminal wave of the 21st century. There is no way we in law enforcement can do it alone.

And that's why today's Summit is so exciting. We are all here today as partners and we have some great opportunities today to gain some new knowledge, some great perspectives, and forge some new partnerships.

Let's come out of this Summit today with stronger than ever partnerships so that we can fight identity theft fraud and get the upper hand over offenders and scams as they continue to evolve.

CONCLUSION:

Today's event would not have been possible without the support of Governor Arnold Schwarzenegger, the State and Consumer Services Agency, its Department of Consumer Affairs, and the event advisory members. Their leadership has allowed for an unprecedented partnership of organizations representing law enforcement, government, businesses, and consumers.

Thank you also to Los Angeles District Attorney Cooley for all of the contributions your office has made to this Summit.

On behalf of the California District Attorneys Association and prosecutors throughout the state, thank you for being a part of *Teaming Up Against Identity Theft: A Summit on Solutions*. I hope that you will enjoy your training classes and find them to be a valuable resource. Thank you all for being a part of this unprecedented event.

|||||

OUR SPONSORS

Deloitte.



GOVERNOR ARNOLD SCHWARZENEGGER

www.governor.ca.gov

CALIFORNIA DISTRICT ATTORNEYS ASSOCIATION

www.cdaa.org

STATE AND CONSUMER SERVICES AGENCY

www.scsa.ca.gov

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

www.dca.ca.gov

CALIFORNIA OFFICE OF PRIVACY PROTECTION

www.privacy.ca.gov

IDENTITY THEFT SUMMIT WEB SITE

www.idtheftsummit.ca.gov

